INVESTIGATION REPORT

NameSilo Called a Crypto Scammer 'The Victim'. Here Are the Receipts.

NameSilo LLC, an ICANN-accredited US domain registrar, publicly defended xmrwallet.com — a documented Monero theft operation — after receiving 20+ abuse reports. Four verifiable lies in four sentences, each rebutted with primary evidence.

#security · #cryptocurrency · #domainnames · #webdev

Canonical source:
https://phishdestroy.eth.limo

Arweave permanent backup (tamper-evident):
https://arweave.net/aHaq6o_GzsMuSEmodv6Wou0tgSe-gL5cREHi-CsarIs

Evidence archive (SHA-256 verified screenshots):
github.com/phishdestroy/namesilo-xmrwallet-coverup

All evidence in this document is released for unrestricted use in legal, regulatory, and law enforcement proceedings. No authorization required. Cite freely.

PUBLISHED BY
PhishDestroy Research
report@phishdestroy.io

PERMANENT ARCHIVE
phishdestroy.eth.limo
github.com/phishdestroy

EVIDENCE LICENSE
Open — cite freely
Legal / regulatory / LE use OK

> *On March 13, 2026, NameSilo LLC (IANA #1479, NASDAQ: CSE:URL) published a Twitter statement about xmrwallet.com — a Monero wallet that had been documented as a private-key theft operation for years. The statement called the site operator "the victim of a hack." It contained four sentences. Four verifiable lies.*

This article documents each lie with primary evidence.

Full investigation: https://phishdestroy.eth.limo

Evidence archive: https://github.com/phishdestroy/namesilo-xmrwallet-coverup

Archived NameSilo statement (immutable): https://ghostarchive.org/archive/CXXZ0

What NameSilo Said

> *"We recently became aware that one of our customer's domains, xmrwallet.com, was compromised a few months ago. Prior to that, we had received no abuse reports about this domain. After an extensive review of this matter, including input from law enforcement but not involving the registrant, we found no basis to terminate the registration. We are currently working with the registrant to remove the website from VT reports."*

Four sentences. Let's go through them.

Lie #1: "The domain was compromised a few months ago"

The claim: xmrwallet.com is a legitimate site that was recently hacked.

The evidence:

The theft mechanism is not a compromise. It is the product. The site's own PHP endpoints encode the user's private view key in the session token (`session_key = [blob]:[base64(address)]:[base64(viewkey)]`), transmit it 40+ times per session, and return `type == 'swept'` — an internal classification that does not exist in the Monero protocol — when funds are swept to the operator's wallet.

This code was built this way. The theft infrastructure predates any alleged "hack" by years. Network captures from 2021, 2022, and 2023 show identical behavior.

The operator's own emails, written before NameSilo's statement, describe the site as his work. He never claimed a hack to PhishDestroy. He claimed the site was legitimate. He defended the code.

Technical proof · **GitHub technical repo**

Lie #2: "We had received no abuse reports about this domain"

The claim: NameSilo had no prior knowledge of xmrwallet.com abuse.

The evidence:

PhishDestroy submitted **20+ delivery-receipted abuse reports** to NameSilo's own abuse portal about xmrwallet.com between 2023 and 2026. Every report has a delivery timestamp. Every receipt is on file.

These are not email guesses. These are reports submitted through NameSilo's official abuse handling system, at the address and in the format their own abuse policy specifies.

NameSilo published their statement claiming no prior reports on March 13, 2026. PhishDestroy submitted the delivery receipts to ICANN Contractual Compliance on March 18, 2026 — five days later.

If NameSilo had no record of 20+ reports with delivery receipts from their own portal, that is not a defense. It is a description of a broken abuse handling process.

Lie #3: "Extensive review... not involving the registrant"

The claim: NameSilo conducted an independent investigation without contacting the operator.

The evidence:

The operator contacted PhishDestroy on **February 16, 2026** — before NameSilo published its statement. In that email, he:

- Defended the site as legitimate
- Claimed no phishing occurred
- Said keys were processed locally (technically false — they are transmitted to the server 40+ times per session)
- Threatened PhishDestroy with legal action

Three days later, on **February 17**, he wrote:

> *"Feel free to subpoena the domain registrar for my information."*

That line was written before any abuse escalation. It describes a registrar relationship he was clearly confident about. Three days later, NameSilo called him "the victim."

Then on **February 23**, same day two of his other domains (.cc and .biz) were suspended by other registrars:

"I've hired a lawyer and a private investigator."

No lawyer appeared. No legal action was filed. The timeline shows a registrant who knew exactly how his registrar would respond.

Operator email Feb 16 · **PhishDestroy reply**

Lie #4: "Working with the registrant to remove the website from VT reports"

The claim: NameSilo is helping clean up a hacked site.

What actually happened: A domain registrar helped an active, documented crypto drainer scrub its security warnings on VirusTotal — while the drainer was still live, while victims were still being robbed.

For comparison, here is what three other registrars did when presented with identical evidence about identical xmrwallet domains:

Registrar	Action	Time to action
PublicDomainRegistry (PDR)	**Suspended**	Days
WebNic	**Suspended**	Days
NICENIC	**DNS killed**	Days
NameSilo	**Wrote a defense. Offered to scrub VirusTotal.**	Never suspended

Same evidence package. Same operator. Four registrars. Three acted. One wrote a press release for the scammer.

The X Lockdown

After PhishDestroy published responses to NameSilo's statement on Twitter/X, the research account — a verified Gold account that had never received a warning — was locked.

- **Email #1 from X Support:** "violation against inauthentic behaviors — will not overturn." No tweet cited. No rule specified. This is a human agent decision after a complaint, not an automated trigger.
- **Email #2 from X Support**, April 15, 2026, subject line **"Your account has been restored"**: "Our automated systems have determined there was no violation and have restored your account to full functionality."

The account remains locked. The Gold subscription continues to be billed. X's automation cleared the account. A human agent overrode it.

X's Gold Checkmark tier — distinct from the $8 blue check — includes direct human support access for paying corporate clients. PhishDestroy's account was locked after a corporate Gold complaint, cleared by automation, then manually re-locked. The posts critical of NameSilo cannot be accessed.

X Support — no violation notice · **X Support — "restored" notice**

The Suppression Pattern

This is not the first time evidence about xmrwallet.com was made to disappear.

Platform	Action taken
GitHub	21+ issues deleted. False DMCA takedowns against repositories.
Trustpilot	Mass-reported negative reviews. 129 reviews deleted in 4 months.
Reddit	60% of r/Monero posts deleted. DMCA/legal threats against victims. 3-person sock puppet network.
BitcoinTalk	Coordinated reporting of warning threads.
YouTube	Technical analysis videos reported and removed.
Google (EU)	GDPR "right to be forgotten" filed to de-index phishdestroy.io from European search results.
Twitter/X	Research account locked via Gold corporate complaint.
SEO	50+ paid articles published to push down victim reports in search.

21+ GitHub issues deleted. Zero technical rebuttals. Zero.

Not one person connected to xmrwallet.com has ever addressed the `session_key` encoding, the `raw_tx_and_hash.raw = 0` return, or the `type == 'swept'` marker. In eight years.

What NameSilo Did Next

After the investigation went public and the evidence reached ICANN, press, and law enforcement channels, xmrwallet.com was **transferred from NameSilo to Namecheap** — with a farewell communication from the operator.

This was not a suspension. NameSilo did not block the domain. The registrar that publicly called this operator "the victim" and offered to scrub his security warnings watched him walk out to a different registrar.

The domain transferred to Namecheap — coincidentally, the registrar PhishDestroy had previously cited as an example of functional abuse handling. PhishDestroy has since filed abuse reports with Namecheap.

Current registrar: verify at https://lookup.icann.org/en/lookup?name=xmrwallet.com

---

What This Means for the Domain Industry

NameSilo is a publicly-traded company (CSE:URL). It is ICANN-accredited. It processes abuse reports from the public. When it receives 20+ documented abuse reports about a site with network-capture-level proof of theft — not allegations, **captures** — and responds by:

1. Claiming it received no reports
2. Calling the operator a victim
3. Offering to clean his security vendor listings

...the question is not whether this was a mistake. The question is what exactly the relationship was.

The ICANN complaint is on file. The receipts are public. The evidence is permanent.

Sources

- **Full investigation:** https://phishdestroy.eth.limo
- **Evidence archive (60+ SHA-256 verified screenshots):** https://github.com/phishdestroy/namesilo-xmrwallet-coverup
- **NameSilo statement (archived):** https://ghostarchive.org/archive/CXXZ0
- **ICANN complaint:** https://www.icann.org/compliance/complaint
- **Trustpilot forensic analysis (7 indicators, 92% manipulation probability):** https://phishdestroy.eth.limo/namesilo-trustpilot.html
- **Permanent Arweave backup:** https://arweave.net/aHaq6o_GzsMuSEmodv6Wou0tgSe-gL5cREHi-CsarIs

Contact: report@phishdestroy.io

All Sources & Permanent Mirrors

Primary investigation site: *https://phishdestroy.eth.limo*

Evidence archive (60+ SHA-256 verified screenshots):
https://github.com/phishdestroy/namesilo-xmrwallet-coverup

Technical GitHub repo (xmrwallet theft code analysis):
https://github.com/phishdestroy/DO-NOT-USE-xmrwallet-com

Arweave permanent backup — tamper-evident, no takedowns:
https://arweave.net/aHaq6o_GzsMuSEmodv6Wou0tgSe-gL5cREHi-CsarIs

IPFS mirror (4everland): *https://ipfs-archive-pbojso5s-phishdestroy.ipfs.4everland.app/*

NameSilo statement (GhostArchive — immutable): *https://ghostarchive.org/archive/CXXZ0*

ICANN Contractual Compliance complaint: *https://www.icann.org/compliance/complaint*

URLScan public records (63+ scans of xmrwallet.com):
https://urlscan.io/search/#domain:xmrwallet.com

VirusTotal: *https://www.virustotal.com/gui/domain/xmrwallet.com*

Contact: *report@phishdestroy.io*